REMARKS

By the foregoing amendment, claims 1, 8 and 13 have been amended. Claims 1-6 and 8-22 are pending in the application. In view of the foregoing amendments and the remarks urged here, Applicant respectfully requests that the Examiner reconsider all outstanding rejections.

35 U.S.C. § 102 Rejections

The Examiner has rejected claims 1, 3-4, 6, 8-10, and 12 under 35 U.S.C. § 102(b) as being anticipated by U.S. Patent No. 5,963,908 to Chadha ("Chadha").

Applicant has amended claims 1 and 8 to more particularly point out and distinctly claim the subject matter regarded as the invention. In particular, claim 1 has been amended to recite the step of "if no previously stored biometric data is stored in said portable computing device, determining if user of said portable computing device is authorized for network use; acquiring new biometric data if the user is authorized for network use; storing said new biometric data." Claim 8 has been amended to recite the step of "if no previously stored biometric data is stored in said portable computing device, determining if user of said portable computing device is authorized for network use; acquiring new biometric data if the user is authorized for network use; storing said new biometric data."

The present invention, as recited in independent claims 1 and 8 is directed to a method and apparatus for controlling access to a computer network where access is controlled by a portable computing device. The problems recognized by embodiments of the present invention is twofold – namely, securing access to a computer network by biometric comparison and securing the portable computing device by biometric comparison. The problem is especially inherent in the use of portable computing devices which are easily stolen or lost. Therefore, the present invention contemplates storage of original biometric data on the computer network and on the portable computing device and if the comparison to the stored biometric data stored fails to identify the authorized user, access to the portable computing device and the computer network is denied. If there is no previously stored biometric data on the portable computing device, the portable computing device, after determining if the user is an authorized user, acquires and stores new biometric data for later authentication of the user. Additionally, the

portable computing device is remotely powered down upon unsuccessful authentication of the biometric data. Finally, if the portable computing device is lost or stolen, the invention contemplates that a remote user (possibly the administrator of the computer network) can remotely delete the original biometric data on the portable computing device preventing unauthorized use of the portable computing device.

By contrast, Chadha is directed to a system and method for controlling user access to stored content and interconnections to various sites accessible through a publicly accessible network. Chadha teaches the use of prestored master voice recognition signals (biometric data) to determine if the user is an authorized user of the network. However, Chadha does not teach or suggest that if there is no previously stored biometric data on the portable computing device, the portable computing device, after determining if the user is an authorized user, acquires and stores new biometric data for later authentication of the user.

Since Chadha does not disclose each and every claim limitation, Applicant respectfully submits that amended claims 1 and 8 are patentable over Chadha. Claims 3-4, 6, 9-10 and 12, by their dependency on amended claims 1 and 8 respectively, are similarly allowable. Early notice to that effect is earnestly solicited.

35 U.S.C. § 103 Rejections

The Examiner has rejected claims 2, 13-14, 17-19, and 21-22 under 35 U.S.C. § 103(a) as being unpatentable over Chadha.

Applicant has amended claims 1, 8, and 13 to more particularly point out and distinctly claim the subject matter regarded as the invention. In particular, claim 1 has been amended to recite the step of "if no previously stored biometric data is stored in said portable computing device, determining if user of said portable computing device is authorized for network use; acquiring new biometric data if the user is authorized for network use; storing said new biometric data." Claim 8 has been amended to recite the step of "if no previously stored biometric data is stored in said portable computing device, determining if user of said portable computing device is authorized for network use; acquiring new biometric data if the user is authorized for network use; storing said new biometric data." Claim 13 has been amended to

recite "a wireless communication device coupled to said computer network, capable of enabling the loading and removing of said biometric data stored in said portable computing device, and wherein said biometric data is operable to be removed from said portable computing device on instruction by one of said one or more workstations on said computer network, said one of said one or more workstations retaining a copy of said biometric data, said wireless communication device configured to determine if user of said portable computing device is authorized for network use and acquiring and storing new biometric data if the user is authorized for network use."

The present invention, as recited in independent claims 1 and 8 is directed to a method and apparatus for controlling access to a computer network where access is controlled by a portable computing device. The problems recognized by embodiments of the present invention is twofold – namely, securing access to a computer network by biometric comparison and securing the portable computing device by biometric comparison. The problem is especially inherent in the use of portable computing devices which are easily stolen or lost. Therefore, the present invention contemplates storage of original biometric data on the computer network and on the portable computing device and if the comparison to the stored biometric data stored fails to identify the authorized user, access to the portable computing device and the computer network is denied. If there is no previously stored biometric data on the portable computing device, the portable computing device, after determining if the user is an authorized user, acquires and stores new biometric data for later authentication of the user. Additionally, the portable computing device is remotely powered down upon unsuccessful authentication of the biometric data. Finally, if the portable computing device is lost or stolen, the invention contemplates that a remote user (possibly the administrator of the computer network) can remotely delete the original biometric data on the portable computing device preventing unauthorized use of the portable computing device.

By contrast, Chadha is directed to a system and method for controlling user access to stored content and interconnections to various sites accessible through a publicly accessible network. Chadha teaches the use of prestored master voice recognition signals (biometric data) to determine if the user is an authorized user of the network. However, Chadha does not teach or

suggest that if there is no previously stored biometric data on the portable computing device, the portable computing device, after determining if the user is an authorized user, acquires and stores new biometric data for later authentication of the user.

The prior art reference (or references) must teach or suggest all of the claim limitations. In re Vaeck, 947 F.2d 488 (Fed. Cir. 1991). Since a prima facie case of obviousness has not been set forth, Applicant respectfully submits that independent claims 1, 8, and 13 are allowable over the cited references. Claims 2, 14, 17-19, and 21-22, by their dependency on claims 1, 8, and 13 respectively, are similarly allowable. Early notice to that effect is earnestly solicited.

Conclusion

All of the stated grounds of rejection have been properly traversed, accommodated, or rendered moot. Applicants therefore respectfully request that the Examiner reconsider all presently outstanding rejections, and that they be withdrawn. The Examiner is invited to telephone the undersigned representative if an interview might expedite allowance of this application.

Respectfully submitted,

BERRY & ASSOCIATES P.C.

Dated: October 15, 2007

By:_____
Bosco Kim
Registration No. 41,896

Berry & Associates P.C.
9255 Sunset Boulevard
Suite 810
Los Angeles, CA 90069
(310) 247-2860